UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: **DEIDRA CLAY**, *individually and on behalf of all others similarly situated*, Plaintiff, v. **CARESOURCE** and **PROGRESS SOFTWARE CORPORATION**, Defendants.	MDL No. 1:23-md-03083-ADB-PGL DIRECT FILED COMPLAINT & JURY DEMAND PURSUANT TO ORDER REGARDING DIRECT FILING CIVIL ACTION NO.

Plaintiff **Deidra Clay** ("Plaintiff"), individually and on behalf of all others similarly situated defined below, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, brings this Amended Class Action Complaint against CareSource and Progress Software Corporation ("PSC") (collectively with CareSource, "Defendants"), and in support thereof alleges as follows:

NATURE OF THE ACTION

1. This Complaint is being directly filed into this MDL proceeding pursuant to the Court's MDL Order No. 12.

2. Plaintiff incorporates the allegations contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

3. Plaintiff brings this class action against Defendants on behalf of herself and all other individuals ("Class Members") who had their Personally Identifiable Information ("PII")

and Protected Health Information ("PHI") (collectively, "Private Information" or "PI") accessed and hacked by malicious, unauthorized third parties that accessed and removed the Private Information from Defendants' systems as early as May 27, 20231 (the "Data Breach").

4. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."2 PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, et seq., as well as multiple state statutes. According to the U.S. Department of Health & Human Services ("HHS"), PHI "is information, including demographic data," that relates to: "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," or "the past, present, or future payment for the provision of health care to the individual," and that "identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual." Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, SSN).3

5. As used throughout this Complaint and previously defined in paragraph 3, "Private Information" is further defined as all information exposed by the Data Breach, including all or any part or combination of name, address, birth date, gender, SSN, member ID, plan name, health condition, medications, allergies, and diagnosis information.

6. This lawsuit seeks to redress the harms caused by CareSource's massive and

[1] Zeba Siddiqui, *Hackers Use Flaw in Popular File Transfer Tool To Steal Data, Researchers Say*, REUTERS (June 2, 2023, 3:43 PM), https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02.

[2] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impactassessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

[3] *See Summary of the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed July 30, 2024).

preventable data breach perpetrated by well-known cybergang, Cl0p ("Clop"). During the data breach Clop infiltrated PSC's inadequately protected MOVEit software that CareSource negligently used and stole the highly sensitive and confidential Private Information Plaintiff and Class Members.

7. Due to Defendants' failure to utilize software with adequate data security measures in place, Plaintiff and the Class face a lifetime risk of fraud and identity theft.

8. CareSource is a managed care organization based in Dayton, Ohio.[4] CareSource administers one of the largest Medicaid managed care plans in the country and offers health insurance to patients.[5] CareSource employs more than 4,700 people and generates more than $11.1 billion in annual revenue.[6]

9. PSC offers both solutions and products, including its file transfer service called MOVEit, which "provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting."[7]

10. CareSource utilizes MOVEit, an automated and managed file transfer software developed by PSC, to transfer Plaintiff's and Class Members' sensitive data between its partners and to prevent unauthorized access to the Private Information when said data is being transferred between entities.

11. On or around May 31, 2023, PSC purportedly discovered a vulnerability in its MOVEit Transfer and MOVEit Cloud systems that "could lead to escalated privileges and potential unauthorized access." On or about that same day, PSC purportedly notified all

[4] *Company Fact Sheet*, CARESOURCE (May 8, 2024), https://www.caresource.com/newsroom/fact-sheets/company-fact-sheet.
[5] *Id.*
[6] *Id.*
[7] *Managed File Transfer Software*, PROGRESS, https://www.progress.com/moveit (last accessed July 30, 2024).

customers, and developed and released a security patch with 48 hours.[8] PSC assigned a severity rating of 9.8 out of 10 to this vulnerability.[9]

12. On September 14, 2023, CareSource sent a letter to Plaintiff and other Data Breach victims (the "Notice Letter"),[10] informing them that:

> **What Happened**
> On May 31, 2023, the software of one of our vendors (MOVEit) was hacked by a bad actor. We use MOVEit software to share data to manage your benefits. We patched the software as instructed by MOVEit on June 1. We then began an investigation to find if any data was stolen.
>
> On June 27, CareSource was named as one of the victims of hacked data. We learned new info at that time. Our investigation found that the bad actor did access the software on May 31. They copied certain data from the server. It also found that the bad actor lost access to the software when the patch was added.
>
> We are sorry to say that some of your protected health information was part of the data stolen by the bad actor.

13. The Notice Letter did not identify the specific data lost for each individual who received the letter. Instead, it said:

> **What Data Was Stolen**
> Our investigation showed that the bad actor may have data like your:
>
> - First Name
> - Last Name
> - Address
> - Date of Birth
> - Gender
> - Social Security Number
> - Member ID
> - Plan Name
> - Health Condition
> - Medications
> - Allergies
> - Diagnosis

[8] *MOVEit Transfer and MOVEit Cloud Vulnerability*, PROGRESS (Jul. 5, 2023), https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability.
[9] Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, EMSISOFT (Jul. 18, 2023), https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.
[10] Exhibit 1.

14. In the Notice Letter, CareSource instructed Plaintiff and Class Members to "[c]heck your accounts for fraudulent activity," "check that your mail from CareSource is correct," and "[l]et us know if any of it seems suspicious." Additionally, CareSoure listed "other steps you can take to protect yourself," like "[a]sk[ing] for a free credit report" or "[a]sk[ing] for a credit freeze or to add a fraud alert on your file."

15. Additionally, CareSource offered Plaintiff and Class Members two free years of credit monitoring through Kroll.

16. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical factors have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

17. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

18. Despite learning of the Data Breach *more than two months* earlier, Defendant did not send the Notice Letter to Plaintiff until on or around September 14, 2023. Thus, cybercriminals were given a head start in misusing Plaintiff's and the Class's PII/PHI before they were even informed of what happened.

19. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and

intrusion.

20. This Complaint is brought against Defendants because of their failure to safeguard the Private Information entrusted to them, and to remedy the harms suffered by Plaintiff and all others similarly situated.

21. Plaintiff and Class Members have suffered injuries as a result of the Defendants' negligent conduct, including: (i) the potential for Plaintiff's and Class Members' exposed Private Information to be sold and distributed on the dark web (if it has not been already), (ii) a lifetime risk of identity theft, sharing, and detrimental use of their sensitive information, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the continued and increased risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to take appropriate and adequate measures to protect their customers' Private Information.

22. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they are entitled to equitable and injunctive relief.

THE PARTIES

23. Plaintiff Deirdra Clay is an adult individual and, at all relevant times herein, a resident and citizen of Ohio, residing in Greenfield, Ohio. Plaintiff is a victim of the Data Breach.

24. Defendant CareSource is a registered nonprofit corporation in Ohio with its headquarters at 230 N. Main Street, Dayton, OH 45402. CareSource is a health plan as that term is defined in 45 C.F.R. 160.103.

25. Defendant PSC is a Delaware corporation and maintains its headquarters and

principal place of business in Burlington, Massachusetts. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

27. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

28. This action was originally filed in the United States District Court for the Northern District of Ohio. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

29. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This case is brought as a class action with an amount in controversy in excess of $5 million, exclusive of interest and costs, there are 100 or more proposed Class Members, and at least one proposed Class Member is a citizen of a state different from Defendant.

30. The United States District Court for the Northern District of Ohio has personal jurisdiction over Defendants because Defendants have sufficient contacts in Ohio, as they conduct a significant amount of business in the state of Ohio.

31. Venue is proper in the United States District Court for the Northern District of Ohio pursuant to 28 U.S.C. § 1391(b)(2) because the injuries in this case substantially occurred in that District, including CareSource collecting and/or storing the Private Information of Plaintiff and Class Members.

COMMON FACTUAL ALLEGATIONS

A. Background

32. Defendant CareSource is a company headquartered in Dayton, Ohio that touts itself as one of the nation's largest Medicaid managed care plans. CareSource offers a number of insurance plans in addition to Medicaid through the Health Insurance Marketplace, and also offers Medicare Advantage plans.[11]

33. CareSource is a sizeable and experienced company, with more than 30 years of experience and more than 4,700 employees serving millions of customers.[12]

34. To provide its services to individuals, CareSource stores, maintains, and uses the Private Information of Plaintiff and the Class Members, including their full name, address, date of birth, gender, Social Security number, member identification number, plan name, health conditions, medications, allergies, and diagnoses.

35. CareSource acknowledges how critical it is to safeguard this information— and, therefore, how devastating it is to individuals whose information has been stolen. CareSource makes the following covenants with its customers:

a. "CareSource employees are trained on how to protect member information."

b. "CareSource makes sure that computers used by employees are safe by using firewalls and passwords."

c. "CareSource limits who can access member health information. We make sure that only those employees with a business reason to access information use and share that information."

d. "We are required by law to keep the privacy and security of your protected health information."

---

[11] *About Us*, CARESOURCE, https://www.caresource.com/about-us/ (last accessed Aug. 3, 2024)

[12] *Company Fact Sheet*, CARESOURCE (May 8, 2024), https://www.caresource.com/newsroom/fact-sheets/company-fact-sheet/.

e. "We will let you know quickly if a breach occurs that may have compromised the privacy or security of your information." [13]

36. PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."14

37. PSC is a Massachusetts-based company that develops and sells a variety of software for businesses, including the secure file transfer application MOVEit. PSC advertises that more than 100,000 enterprises run business systems through its platforms, and 6 million business users work with apps running on PSC's technologies.[15]

38. PSC's various business and government customers retain sensitive information including, but not limited to, bank account information, addresses, driver's license numbers, dates of birth, and social security numbers, and use PSC's MOVEit product to securely transfer files containing that sensitive information.

39. While administering these services, PSC receives, handles, and collects consumer PII, which includes, *inter alia*, names, addresses, dates of birth, and Social Security numbers.

40. By obtaining, collecting, and storing Plaintiff's and the Class Members' PII, PSC knew, or should have known, that it was a prime target for hackers given the significant amount of sensitive personal information processed through its customers' computer data and storage systems. PSC's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

---

[13] *See, e.g.*, *HIPAA Privacy Practices – Ohio Medicaid*, CARESOURCE, https://www.caresource.com/about-us/legal/hipaa-privacy-practices/hipaa-privacy-practices-ohio-medicaid/ (last accessed Aug. 3, 2024).

[14] *Company*, PROGRESS, htttps://progress.com/company (last accessed July 31, 2024).

[15] *Company Overview*, PROGRESS, https://investors.progress.com/ (last visited Aug. 16, 2024).

41. On or around May 31, 2023, PSC's MOVEit software, which Defendant uses to share Class Members' data in order to manage their benefits was hacked by a malicious actor.[16]

42. CareSource states that it patched its software on June 1, 2023—the day after the breach.[17] This was too little and too late.

43. PSC reports that it alerted users of its software to take down traffic to MOVEit software "[p]romptly following discovery and escalation of the vulnerability" on May 30, 2023, and it published and released the patch on May 31, 2023.[18]

44. CareSource began an investigation on June 1, 2023, to determine whether information was stolen. By June 27, 2023, it was confirmed that data in CareSource's custody had been breached.[19]

45. Despite its promise to customers that "We will let you know quickly if a breach occurs that may have compromised the privacy or security of your information,"[20] CareSource did not send victims of the Data Breach a Notice of Data Breach Letter until more than two months later, on or about September 14, 2023.

46. The Notice Letter CareSource sent admits that Plaintiff's and Class Members' Private Information was accessed by cybercriminals without authorization.

47. Cl0p accessed and acquired files in Defendants' computer systems containing the unencrypted PI of Plaintiff and Class Members.

48. CareSource utilized PSC's file transfer service, MOVEit, as a web transfer

[16] *See* Exhibit 1.
[17] *See* Exhibit 1.
[18] *Status of the May 2023 Security Vulnerability and Defensive Outage of MOVEit Cloud*, PROGRESS (June 1, 2023), https://community.progress.com/s/article/MOVEit-Cloud-Info-Regarding-Critical- Vulnerability-May-2023.
[19] *See* Exhibit 1.
[20] *See, e.g.*, *HIPAA Privacy Practices – Ohio Medicaid*, CARESOURCE, https://www.caresource.com/about-us/legal/hipaa-privacy-practices/hipaa-privacy-practices-ohio-medicaid/ (last accessed Aug. 3, 2024).

application to transfer documents. CareSource utilized the software with disregard for its data security and infrastructure.

49. Defendants agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws. Defendants had obligations created by the FTC Act, HIPAA, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

50. To this end, CareSource acknowledged that "[w]e are required by law to keep the privacy and security of your protected health information." Similarly, as incorporated and realleged herein, Progress knew of its obligations to protect Plaintiff's and Class Members' Private Information, including of industry cybersecurity standards, and could have prevented the Data Breach by following industry standards for secure software development and maintenance. *See* ECF No. 908 (sections III-IV).

51. Defendants knew of their duties to Plaintiff and the Class Members, and the risks associated with failing to protect the Private Information entrusted to them. In particular, CareSource knew that if it did not select a vendor/software with adequate security, it put Plaintiff's and the Class's Private Information at risk for unlawful exposure.

52. Defendants also knew that if they did not properly monitor and secure the systems under their own control, including the MOVEit software and related systems and servers, the PI with which they were entrusted could be breached.

53. Upon information and belief, Defendants failed to reasonably secure their systems handling consumers' PI, including the MOVEit software PSC hosted. CareSource also unreasonably failed to monitor and oversee PSC's data security throughout CareSource's use of

the MOVEit software. Had Defendants acted reasonably with respect to this critically sensitive PI, Plaintiff's and the Class's Private Information would have never been exposed in the Data Breach.

54. The unencrypted Private Information of Plaintiff and Class Members will likely be, or already is, for sale on the dark web, and may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can already access the Private Information of Plaintiff and Class Members.[21]

55. Defendants were negligent and did not use or implement reasonable security procedures, oversight, and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PI for Plaintiff and Class Members.

56. Defendants were also negligent in that they did not use, develop, or maintain software with adequate data security. In particular, CareSource should have inquired about MOVEit's data security prior to entrusting Plaintiff's and the Class's PI to PSC as a vendor.

57. Because Defendants had a duty to protect Plaintiff's and Class Members' Private Information, Defendants should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

58. In October 2019, the Federal Bureau of Investigation published an article online

[21] Alex Scroxton, *Clop Cyber Gang Claims MOVEit Attack and Starts Harassing Victims*, COMPUTER WEEKLY (June 7, 2023, 12:00 PM), https://www.computerweekly.com/news/366539357/Clop-cyber-gang-claims- MOVEit-attack-and-starts-harassing-victims; Naomi Eide, *Clop Names a Dozen MOVEit Victims, but Holds Back Details*, CYBERSECURITY DIVE (June 15, 2023), https://www.cybersecuritydive.com/news/clop-moveit-data-leaks-victims-named/ 653131/.

titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[22]

59. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[23]

60. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[24]

61. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that: (i) cybercriminals were targeting big companies such as Defendants and Defendants' clients, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendants and Defendants' clients, (iii) cybercriminals were leaking corporate information

[22] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002 (emphasis added).

[23] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware- mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Sept. 20, 2023).

[24] *Ransomware Guide*, CISA (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

62. Considering the information readily available and accessible on the internet before the Data Breach and Defendants' involvement in data breach litigation, CareSource, having elected to store the unencrypted Private Information of Plaintiff and Class Members with PSC without first ensuring that PSC's system was secure, had reason to know that Plaintiff and the Class Members' Private Information was at risk for being shared with unknown and unauthorized persons.

63. Prior to the Data Breach, CareSource knew or should have known that it was responsible for confirming that MOVEit's systems were secure and capable of protecting Plaintiff's and the Class Members' Private Information.

64. Similarly, PSC should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cyber criminals looking to steal Private Information. Therefore, PSC should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the Data Breach.

65. Since the Data Breach, Defendants continue to store confidential information, including Plaintiff's and Class Members' Private Information, and have failed to give adequate assurances that they have enhanced their security practices sufficiently to avoid another breach in the future.

B. Plaintiff Deidra Clay's Experience

66. Plaintiff Deidra Clay received health insurance through CareSource for approximately four or five years until her coverage stopped in or around March 2024.

67. At all times herein relevant, Plaintiff is and was a member of each of the

Classes.

68. In order to obtain services from CareSource, Plaintiff provided CareSource with highly sensitive Private Information that it then possessed and controlled. Because CareSource provides managed care services for Plaintiff Clay's healthcare, the Private Information she provided pertained both to her doctor visits and to her prescriptions.

69. CareSource, in turn, negligently used PSC's MOVEit software to transfer files containing Plaintiff's PI. Defendants were in possession of Plaintiff's Private Information before, during, and after the Data Breach.

70. Plaintiff received a Notice Letter about the Data Breach on or around September 14, 2023. The Notice Letter stated that the information exposed in the breach included Plaintiff's full name, address, date of birth, gender, Social Security number, member identification number, plan name, health conditions, medications, allergies, and diagnoses.

71. Plaintiff was unaware of the Data Breach—or even that Defendants had retained possession of her data—until receiving that letter.

72. As a result of the Data Breach, Plaintiff was forced to spend time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice of Data Breach, researching the Data Breach, self-monitoring her accounts, changing the passwords on several of her accounts, investigating fraudulent activity, and contacting banks about fraudulent activity. This time has been lost forever and cannot be recaptured.

73. Plaintiff has also experienced actual misuse of her Private Information. Since the Data Breach, Plaintiff received several alerts that she did not have funds to cover a purchase despite the fact that she was not making any purchases. She contacted her bank to cancel her card and get a new card twice as a result of these fraudulent charge attempts.

74. Plaintiff also received an Amazon two-factor notification asking her to approve a log-in attempt, even though she had not been trying to log in to her account. Plaintiff had to change her Amazon password as a result.

75. Additionally, after the breach, Plaintiff experienced a significant increase in spam text messages, emails, physical mail, and calls to her landline and cell phone. Because Plaintiff is required by her work to be responsive to phone calls and cannot simply ignore them, these spam calls impose a significant interruption to Plaintiff's daily life.

76. The misuse of Plaintiff's Private information has caused her significant frustration and anxiety.

77. Plaintiff is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

78. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (i) lost time related to monitoring her accounts for fraudulent activity; (ii) loss of privacy due to her Private Information being exposed to cybercriminals; (iii) loss of the benefit of the bargain because Defendants did not adequately protect her Private Information; (iv) emotional distress because identity thieves now possess her Private Information; (v) exposure to increased and imminent risk of fraud and identity theft now that her Private Information has been exposed; (vi) the loss in value of her Private Information due to her Private Information being in the hands of cybercriminals who can use it at their leisure; and (vii) other economic and non-economic harm.

79. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private

Information being placed in the hands of unauthorized third parties and criminals.

80. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

C. Cyber Criminals Will Use Plaintiff's PI to Defraud Her

81. PI is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members to profit off their misfortune.

82. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[25] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[26] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

83. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in

[25] *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last accessed Aug. 5, 2024) (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[26] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, USA TODAY (Nov. 15, 2017, 4:00 PM), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity- thief-can-use-your-social-security-number/860643001/.

> bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways. [27]

84. PI are such valuable commodities to identity thieves that once this information has been compromised, criminals will use it for years.[28]

85. This Data Breach was financially motivated, as the reason the cyber criminals go through the trouble of running a targeted cyberattack is to get information that they can monetize by selling it on the black market for use in the kinds of criminal activity described herein. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[29] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[30]

86. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PI, they ***will*** use it.[31]

87. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[32]

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

---

[27] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/ (emphasis added).
[28] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737.
[29] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, SEC. WATCH (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[30] *Dark Web Monitoring: What You Should Know*, CONSUMER FED. OF AM. (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/.
[31] Ari Lazarus, *How Fast Will Identity Thieves Use Stolen Info?*, MIL. CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[32] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 4, 2007), https://www.gao.gov/assets/gao-07-737.pdf.

88. For instance, with a stolen Social Security number, which is part of the PI compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[33]

89. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' PI secure are long-lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for up to six to twelve months, or even longer.

90. Approximately 11% of victims do not realize their identity has been compromised for more than a month, and 6% of victims do not discover the fraud for more than a year.[34]This gives thieves ample time to commit multiple fraudulent activities, including seeking medical treatment under the victim's name.

91. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

92. Defendants' offer of two years of identity monitoring and protection services to Plaintiff and the Class is woefully inadequate and will not fully protect them from the damages and harm caused by Defendants' cybersecurity failures. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the twenty-four months have expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to

[33] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, USA TODAY (Nov. 15, 2017, 4:00 PM), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity- thief-can-use-your-social-security-number/860643001/.

[34] Rob Lever, *U.S. News & World Report Identity Theft Survey 2023*, U.S. NEWS (Sept. 12, 2023), https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey.

Defendant's negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PI)—it does not prevent identity theft.[35] Nor can an identity monitoring service remove personal information from the dark web.[36] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[37]

93. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach in their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and Class Members must take.

94. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

---

[35] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be- worth-the-cost.html.

[36] *Dark Web Monitoring: What You Should Know*, CONSUMER FED. OF AM. (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/.

[37] *Id.*

a. Trespass, damage to, and theft of their personal property including PI;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

d. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves may use that information to defraud other victims of the Data Breach;

e. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach; and

f. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' Private Information for which there is a well-established and quantifiable national and international market.

95. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendants, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendants have shown themselves wholly incapable of protecting Plaintiff's and Class Members' Private Information.

96. Defendants acknowledged the harm caused by the Data Breach because they offered Plaintiff and Class Members the woefully inadequate twenty-four months of identity monitoring and protection services. Twenty-four months of identity monitoring and protection

services is, however, insufficient to protect Plaintiff and Class Members from a lifetime of identity theft risk.

97. CareSource further acknowledged in the Notice Letter that it needed to improve its security protocols, stating: "We are doing a full investigation and are looking into what, if any, updated processes may be needed."[38]

98. The Notice Letter further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, telling Class Members to "Stay alert. Check your accounts for fraudulent activity."[39]

99. At Defendants' suggestion, Plaintiff and Class Members are desperately trying to mitigate the damage that Defendants' Data Breach has caused them. Given the kind of Private Information Defendants made accessible to hackers by utilizing inadequate security measures, Plaintiff and Class Members are certain to incur additional damages. Because identity thieves have their PI, Plaintiff and Class Members will need to have identity monitoring and protection services for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[40]

100. None of this should have happened.

D. Defendants Were Aware of the Risk of Cyber Attacks

101. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of

[38] *See* Exhibit 1.
[39] *Id.*
[40] *What Happens If I Change My Social Security Number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

some of the biggest cybersecurity breaches: Target,[41] Yahoo,[42] Marriott International,[43] Chipotle, Chili's, Arby's,[44] and others.[45]

102. CareSource, which provides managed care services to companies throughout the United States requiring the collection and maintenance of highly sensitive and valuable PI, should certainly have been aware, and indeed was aware, that failing to ensure the MOVEit software employed minimum basic security precautions created a substantial risk for a data breach that could expose the Private Information it collected and maintained.

103. Similarly, PSC failed to identify and remediate vulnerabilities in its MOVEit software and secure Plaintiff's and Class Members' Private Information despite its duties to do so, although it knew or should have known of the vulnerabilities in its software and that it was obligated to patch them. *See* ECF No. 908 (section IV).

104. With the increasing prevalence of data breach announcements, Defendants certainly recognized they had a duty to use reasonable measures to protect the wealth of PI they collected and maintained.

105. In 2022, a total of 1,802 data breaches occurred, which represents the second highest number of data events in a single year and just 60 events short of the all-time record of 1,862 in 2021.[46]

---

[41] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015, 8:29 AM), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[42] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the- russian-hack-of-yahoo-how-they-did-it.html.

[43] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach- this-is-why-insurance-matters/.

[44] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in- theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[45] *See, e.g.*, Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data- breaches-of-the-21st-century.html.

[46] *2022 Data Breach Report*, ID THEFT CENTER, https://www.idtheftcenter.org/wp-

106. In light of the significant number of data breaches that occurred in 2022, Defendants knew or should have known that their customers' Private Information would be targeted by cybercriminals.

107. Defendants were clearly aware of the risks they were taking when they failed to ensure the MOVEit software provided sufficient cybersecurity protection, and of the harm that could result from inadequate data security.

E. Defendants Could Have Prevented the Breach

108. Data breaches are preventable.[47] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[48] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[49]

109. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[50]

110. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing

content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last accessed Aug. 5, 2024).
47 Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[48] *Id.* at 17.
[49] *Id.* at 28.
[50] *Id.*

risks to computer systems, and implementing safeguards to control such risks.[51] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

111. Upon information and belief, Defendants failed to ensure that the MOVEit software maintained reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendants also failed to ensure that the MOVEit software met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity preparation.

112. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[52]

113. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

---

[51] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal- information.pdf.

[52] *See* HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE at 3, F B I , https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/ view (last accessed Aug. 5, 2024)..

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. [53]

114. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

> **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
>
> **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (*e.g.*, contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (*e.g.*, .com instead of .net)….
>
> **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
>
> **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current

[53] *Id.* at 3-4.

> Activity, or Tip has been published.
>
> **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[54]

115. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:[55]

a. Secure internet-facing assets

   1) Apply latest security updates

   2) Use threat and vulnerability management

   3) Perform regular audit; remove privileged credentials

b. Thoroughly investigate and remediate alerts

   1) Prioritize and treat commodity malware infections as potential full compromise;

c. Include IT Pros in security discussions

   1) Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

d. Build credential hygiene

   1) Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

[54] *See Security Tip (ST19-001) Protecting Against Ransomware*, CISA (Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware.

[55] *See* Microsoft Threat Intelligence, *Human-Operated Ransomware Attacks: A Preventable Disaster*, MICROSOFT (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated- ransomware-attacks-a-preventable-disaster/.

e. Apply principle of least-privilege

1) Monitor for adversarial activities

2) Hunt for brute force attempts

3) Monitor for cleanup of Event Logs

4) Analyze logon events

f. Harden infrastructure

1) Use Windows Defender Firewall

2) Enable tamper protection

3) Enable cloud-delivered protection

4) Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

116. Given that Defendants utilized the MOVEit transfer tool to store the Private Information of thousands of individuals, including Plaintiff and the Class Members, Defendants could and should have ensured that the MOVEit software was capable of preventing and detecting cyber-security attacks.

117. To prevent zero-day attacks, Defendants could and should have implemented, as recommended by Security Intelligence, the following:

> **Patch management:** Formal patch management can help security teams remain aware of critical patches.
>
> **Vulnerability management:** Vulnerability assessments and penetration tests can help companies detect zero-day vulnerabilities before adversaries find them.
>
> **Attack surface management (ASM):** ASM enables security teams to identify all network assets and scan them for vulnerabilities. ASM tools assess the network from an attacker's perspective, focusing on how threat actors might try to exploit assets.

> **Threat intelligence:** Security researchers are often the first to identify zeroday vulnerabilities. Organizations that receive threat intelligence updates may be informed about zero-day vulnerabilities sooner.
>
> **Anomaly-based detection methods**: Machine learning tools can spot suspicious activity in real-time. Common anomaly-based detection solutions include user and entity behavior analytics (UEBA), extended detection and response (XDR) platforms, endpoint detection and response (EDR) tools and some intrusion detection and intrusion prevention systems.[56]

118. Defendants acquired, collected, and stored the Private Information of Plaintiff and Class Members.

119. Plaintiff and other Members of the Class entrusted their Private Information to Defendants.

120. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PI from disclosure.

121. Given that Defendants were storing the Private Information of other individuals, Defendants could and should have implemented all of the above measures to prevent and detect cyber-security attacks.

122. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

123. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and data fields containing the Private Information of Plaintiff and

[56] *See* Jonathan Reed, *The MOVEit Breach Impact and Fallout: How Can You Respond?*, SEC. INTEL. (July 19, 2023), https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

Class Members and ensuring the MOVEit software properly secured and encrypted the folders, files, and/or data fields containing the Private Information of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data that it no longer had a reasonable need to maintain, or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

124. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

125. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

F. Defendants' Response to and Notice of the Data Breach is Inadequate to Protect Plaintiff and the Class

126. Defendants failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

127. CareSource stated that "[o]n May 31, 2023, the software of one of our vendors was hacked by a bad actor. We use MOVEit software to share data to manage your benefits. We patched the software as instructed on June 1."[57] Further, by June 27, 2023, CareSource confirmed that its customers' data had been hacked.[58] Despite the public notices published by PSC, and CareSource's awareness of its use of PSC's MOVEit tool, CareSource did not notify Plaintiff until on or about September 14, 2023 —over two months after CareSource had definitive

[57] *See* Exhibit 1.
[58] *Id.*

knowledge of the breach.

128. During these intervals, the cybercriminals had the opportunity to exploit Plaintiff's and Class Members' Private Information while Defendants were sitting idle.

G. Defendants Failed to Comply with FTC Guidelines

129. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

130. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[59] The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[60]

131. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must

[59] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal- information.pdf..
[60] *Id.*

take to meet their data security obligations.

132. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.

133. Defendants were always fully aware of their obligations to protect the Private Information of Plaintiff and Class Members and the significant repercussions that would result from its failure to ensure the MOVEit software had adequate data security.

H. Defendants Failed to Adhere to HIPAA

134. Defendants had specific obligations imposed on them by contracts and law to ensure the adequate protection of such information. For example, as a covered entity under HIPAA, CareSource was required to maintain the confidentiality and security of Plaintiffs' and Class Members' Private Information. Similarly, as a Business Associate to Covered Entities, Progress was required to comply with HIPAA as well.

135. Defendants are regulated by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendants' protection of medical information maintained in electronic form.

136. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

137. "Electronic protected health information" is defined as "individually

identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

138. HIPAA's Security Rule requires Defendants to: "(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business as-sociate creates, receives, maintains, or transmits; (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted . . . ; and (d) Ensure compliance . . . by its workforce." 45 C.F.R. § 164.306(a).

139. HIPAA also requires Defendants to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1).

140. The facts of the Data Breach establish that Defendants failed to comply with these Rules. The Data Breach resulted from a combination of inadequacies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii);

e. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4);

h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, et seq.;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to

carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. §§ 164.530(b) and 164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. § 164.530(c).

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this class action individually on behalf of herself and on behalf of the Nationwide Classes, defined below. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and, as appropriate, (c)(4) of the following Classes:

CareSource Nationwide Class

All persons in the United States who provided their Private Information to CareSource whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by CareSource.

Progress Nationwide Class

All persons in the United States whose Private Information was compromised in the MOVEit Data Breach.

142. Pursuant to Fed. R. Civ. P. 23(a), (b)(3), and (c)(4), Plaintiff brings this action on behalf of herself and on behalf of subclasses for residents of Ohio ("Ohio Subclasses"), defined below, and seeks certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims (Counts XII-XIII).

CareSource Ohio Subclass

All persons residing in the state of Ohio who provided Private Information to CareSource whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by CareSource.

Progress Ohio Subclass

All persons residing in the state of Ohio whose Private Information was compromised in the MOVEit Data Breach.

143. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

144. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

145. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

146. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Plaintiff Classes (which Plaintiff is informed and believes, and on that basis, alleges that the total number of persons is in the thousands of individuals and can be determined analysis of Defendants' records) are so numerous that joinder of all members is impractical, if not impossible.

147. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not limited to:

a. Whether Defendants had a legal duty to Plaintiff and the Classes to

exercise due care in collecting, storing, using, and/or safeguarding their PI;

b. Whether Defendants knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PI had been compromised;

g. How and when Defendants actually learned of the Data Breach;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the PI of Plaintiff and Class Members;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendants' wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

148. Typicality: Plaintiff's claims are typical of the claims of the Plaintiff Classes. Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

149. Adequacy of Representation: Plaintiff in this class action is an adequate

representative of each of the Plaintiff Classes in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

150. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Plaintiff anticipates no management difficulties in this litigation.

151. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

152. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

153. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

154. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on

Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

155. Unless a Class-wide injunction is issued, Defendants may continue failing to properly secure the PI of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

156. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Federal Civil Procedure Rule 23(b)(2).

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

157. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

158. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty of care, inter alia, to act with reasonable care to secure and safeguard their PI and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PI of Plaintiff and Class Members in their computer systems and on their networks.

159. Among these duties, Defendants were expected to:

a) exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PI in its possession;

b) protect Plaintiff's and Class Members' PI using reasonable and adequate

security procedures and systems that were/are compliant with industry-standard practices;

c) implement processes to detect a data breach quickly and to timely act on warnings about data breaches; and

d) promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PI.

160. Defendants knew that the PI was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

161. Defendants knew, or should have known, of the risks inherent in collecting and storing PI, the vulnerabilities of their data security systems, and the importance of adequate security.

162. Defendants knew about numerous, well-publicized data breaches.

163. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PI.

164. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PI that Plaintiff and Class Members had entrusted to them.

165. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PI.

166. Because Defendants knew that a breach of their systems could damage thousands of individuals, including Plaintiff and Class Members, Defendants had a duty to

adequately protect their data systems and the PI contained therein.

167. Plaintiff's and Class Members' willingness to entrust Defendants with their PI was predicated on the understanding that Defendants would take adequate security precautions.

168. Moreover, only Defendants had the ability to protect their systems and the PI is stored on them from attack. Thus, Defendants had a special relationship with Plaintiff and Class Members.

169. Defendants also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PI and promptly notify Plaintiff and Class Members about the Data Breach. These "independent duties" are untethered to any contract between Defendants, Plaintiff, and/or the remaining Class Members.

170. Defendants breached their general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PI of Plaintiff and Class Members;

b) by failing to timely and accurately disclose that Plaintiff's and Class Members' PI had been improperly acquired or accessed;

c) by failing to adequately protect and safeguard the PI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PH;

d) by failing to provide adequate supervision and oversight of the PI with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown

third party to gather PI of Plaintiff and Class Members, misuse the PI. and intentionally disclose it to others without consent.

e) by failing to adequately train their employees not to store PI longer than absolutely necessary;

f) by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PI;

g) by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h) by failing to encrypt Plaintiff's and Class Members' PI and monitor user behavior and activity in order to identify possible threats.

171. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

172. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages.

173. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PI to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PI.

174. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

175. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Plaintiff and Class Members.

176. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI.

177. There is a close causal connection between Defendants' failure to implement security measures to protect the PI of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

178. Plaintiff's and Class Members' PI was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PI by adopting, implementing, and maintaining appropriate security measures.

179. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

180. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

181. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PI is used; (iii) the compromise, publication, and/or theft of their PI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach,

including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PI, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PI in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

182. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

183. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

184. Defendants' duties arise from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

185. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as

interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private Information.

186. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtain and store, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

187. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

188. Plaintiff and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

189. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

190. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

191. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section

5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

192. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

193. Through its course of conduct, Defendants, Plaintiff and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PI.

194. CareSource required Plaintiff and Class Members to provide and entrust their PI as a condition of obtaining its services.

195. CareSource solicited and invited Plaintiff and Class Members to provide their PI as part of CareSource's regular business practices.

196. Plaintiff and Class Members accepted CareSource's offers and provided their PI to CareSource.

197. As a condition of being direct customers of CareSource, Plaintiff and Class Members provided and entrusted their PI to it.

198. In so doing, Plaintiff and Class Members entered into implied contracts with CareSource by which CareSource agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

199. Upon accepting Plaintiff's and Class Members' Private Information, CareSource provided Plaintiff's and Class Members' Private Information to PSC in the course of using PSC's MOVEit software.

200. Privacy Policies and Practices of CareSource assure Plaintiff and Class Members of its practice to safeguard their Private Information and of its legal obligation to do so.

201. Defendants accepted and maintained the Private Information of Plaintiff and Class Members that they acquired either from CareSource or direct receipt from Plaintiff and Class Members, and thus monetarily benefitted from Plaintiff and Class Members providing their Private Information, and thus Plaintiff and Class Members entered into implied contracts with CareSource's business associates and file transfer software providers, including PSC.

202. Alternatively, Plaintiff and Class Members were the intended beneficiaries of Business Associate Agreements entered into between CareSource and its business associates, including PSC, which governed PSC's use, disclosure, and transfer terms.

203. In entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that CareSource's, and their associates', including Progress's, data security practices complied with relevant laws and regulations and were consistent with industry standards, and that they would thoroughly vet and select vendors that adequately protect Private Information.

204. A meeting of the minds occurred when Plaintiff and Class Members agreed to,

and did, provide their PI to Defendants, in exchange for, amongst other things, the protection of their PI.

205. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

206. Defendants breached their implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PI and by failing to provide timely and accurate notice to them that their PI was compromised as a result of the Data Breach.

207. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

FOURTH CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of the Nationwide Class and the Ohio Subclass against PSC)

208. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

209. PSC entered into contracts with its government and corporate customers to provide services to them using MOVEit; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to Defendants.

210. Such contracts were made expressly for the benefit of Plaintiff and the Class

Members, as it was their Private Information that Defendants agreed to receive, store, utilize, transfer, and protect through their services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class Members was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

211. PSC knew or should have known that if it were to breach these contracts, Plaintiff and Class Members would be harmed.

212. PSC breached its contracts by, among other things, failing to adequately secure Plaintiff's and Class Members' Private Information, and, as a result, Plaintiff and Class Members were harmed by PSC's failure to secure their Private Information.

213. As a direct and proximate result of the Data Breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in PSC's control, and which is subject to further breaches, so long as PSC fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

214. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

215. Plaintiff and Class Members are also entitled to injunctive relief requiring PSC to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH CAUSE OF ACTION
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

216. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

217. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

218. Plaintiff and Class Members have complied with and performed all conditions of their express or implied contracts with Defendants.

219. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PI, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continuing to accept and store Private Information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

220. Defendants acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

SIXTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

221. Plaintiff realleges and reincorporates every allegation set forth in paragraphs 1-156 as though fully set forth herein.

222. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

223. Defendants, prior to and at the time Plaintiff and Class Members entrusted their PI to CareSource for the purpose of obtaining health services, caused Plaintiff and Class Members to reasonably believe that Defendants would keep such PI secure.

224. Defendants were aware, or should have been aware, that reasonable patients and consumers would have wanted their PI kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

225. Defendants were also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

226. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

227. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Plaintiff and Class Members the ability to make a rational and informed decision and took undue advantage of Plaintiff and Class Members.

228. Defendants were unjustly enriched at the expense of Plaintiff and Class

Members, as Defendants received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

229. Since Defendants' profits, benefits, and other compensation were obtained improperly, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits they realized from these transactions.

230. Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

SEVENTH CAUSE OF ACTION
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

231. Plaintiff incorporates by reference all preceding factual allegations in paragraphs 1-156 as though fully alleged herein.

232. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

233. Defendants' negligent, reckless, and intentional conduct as alleged herein intruded upon Plaintiff's and Class Members' seclusion under common law.

234. By intentionally and/or knowingly failing to keep Plaintiff's and Class Members' Private Information safe, and by knowingly misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants negligently, recklessly, and

intentionally invaded Plaintiff's and Class Members' privacy by intruding into Plaintiff's and Class Members' private affairs, without approval, in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities.

235. Defendants knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendants' negligent, reckless, and intentional actions highly offensive and objectionable.

236. Such an intrusion into Plaintiff's and Class Members' private affairs is likely to cause outrage, shame, and mental suffering because the Private Information disclosed contained PII and PHI.

237. Defendants invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

238. The Private Information disclosed by Defendant has no legitimate reason to be known by the public.

239. Defendants intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

240. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests, caused anguish and suffering such

that a person with ordinary sensibilities would consider Defendants' intentional actions or inaction highly offensive and objectionable.

241. In failing to protect Plaintiff's and Class Members' Private Information, and in negligently, recklessly, and intentionally misusing and/or disclosing their Private Information, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

EIGHTH CAUSE OF ACTION
INVASION OF PRIVACY – PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of the Nationwide Class and the Ohio Subclass against PSC and CareSource)

242. Plaintiff realleges and incorporates by reference the allegations contained in the paragraphs 1-156 as if fully set forth herein.

243. Plaintiff and Class Members reasonably expected that the highly personal, sensitive Private Information entrusted to Defendants, directly or indirectly, would be kept private, confidential, and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

244. Defendants unlawfully invaded the privacy rights of Plaintiff and Class Members by:

a. Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c. Enabling the disclosure of their personal and sensitive Private Information without their informed, voluntary, affirmative, and clear

consent.

245. Plaintiff's and Class Members' Private Information, such as health information and Social Security numbers, that was publicized due to the Data Breach, was highly sensitive, private, confidential, and of no general public interest, and a reasonable person would consider its publication highly offensive and egregious.

246. A reasonable person would find it highly offensive that Defendants, having collected Plaintiff's and Class Members' sensitive Private Information, directly or indirectly, in a commercial transaction, failed to protect such Private Information from unauthorized disclosure to third parties.

247. In failing to adequately protect Plaintiff's and Class Members' sensitive Private Information, Defendants acted in reckless disregard of Plaintiff's and Class Members' privacy rights. CareSource knew or should have known that its ineffective security measures, including the failure to verify and validate the security practices of its vendor, PSC, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and Class Members' position. PSC knew or should have known of the risks of failing to implement adequate data security practices too, and the foreseeability and offensiveness of such disclosures.

248. Defendants violated Plaintiff's and Class Members' right to privacy under the common law.

249. Defendants' unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of Defendants' unlawful invasion of privacy and public disclosure of private facts, Plaintiff's and Class Members' reasonable expectations of privacy were frustrated and defeated. Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b)

financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out-of-pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

250. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach and these invasions of privacy.

251. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, inter alia: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

NINTH CAUSE OF ACTION
BREACH OF CONFIDENTIALITY
(On Behalf of Plaintiff and the Ohio Subclass against CareSource)

252. Plaintiff incorporates by reference all preceding factual allegations in paragraphs 1-156 as though fully alleged herein.

253. At all times during Plaintiff's and Class Members' interactions with CareSource, CareSource was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

254. Plaintiff's and Class Members' Private Information constitutes confidential and

novel information. For example, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Similarly, Plaintiff and Class Members cannot change their medical histories.

255. As alleged herein and above, CareSource's relationships with Plaintiff and Class Members were governed by terms and expectations that Plaintiff's and Class members' Private Information would be collected, stored, and protected in confidentiality, and would not be disclosed to unauthorized third parties.

256. Plaintiff and Class Members provided their respective Protected Information to CareSource with the explicit and implicit understandings that CareSource would protect and not permit the Private Information to be disseminated to any unauthorized parties.

257. CareSource voluntarily received in confidentiality Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

258. Due to CareSource's failure to ensure the MOVEit software was capable of preventing, detecting, and avoiding the Data Breach from occurring by, inter alia, not following best information security practices and by not providing proper training to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

259. As a direct and proximate cause of CareSource's actions and/or omissions, Plaintiff and Class Members have suffered damages.

260. But for CareSource's disclosure of Plaintiff's and Class Members' Private Information through its use of unsecured systems in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. CareSource's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

261. This disclosure of Plaintiff's and Class Members' Private Information constituted a violation of Plaintiff's and Class Members' understanding that CareSource would safeguard and protect the confidential and novel Private Information that Plaintiff and Class Members were required to disclose to CareSource.

262. The concrete injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of CareSource's unauthorized disclosure of Plaintiff's and Class Members' Private Information. CareSource knew or should have known that the MOVEit software's data security measures had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' Private Information in jeopardy.

263. As a direct and proximate result of CareSource's breaches of confidentiality, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PI; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PI, which remains in CareSource's possession and is subject to further unauthorized disclosures so long as CareSource fails to take appropriate and adequate measures to protect the Private Information under its continued control; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

TENTH CAUSE OF ACTION
VIOLATION OF MASSACHUSETTS GENERAL LAWS, Chapter 93A
(On behalf of the Nationwide Class and the Ohio Subclass against PSC)

264. Plaintiff realleges and incorporates by reference paragraphs 1-156 as if fully set forth herein.

265. M.G.L. ch. 93A §§ 2 and 9. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

266. Plaintiff alleges that PSC committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

267. PSC knew or should have known of the inherent risks in experiencing a data breach if it failed to maintain adequate systems and processes for keeping Plaintiff's and Class members' Private Information safe and secure. Only PSC was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and the Class resulting from a data security incident such as the Data Breach; instead, it failed to implement such safeguards.

268. PSC's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. PSC's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

269. PSC acknowledges its conduct created actual harm to Plaintiff and Class members because Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft.

270. PSC knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, inter alia, the prevalence of data breaches.

271. PSC failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff and Class members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiff and Class members in a timely manner that their Private Information was accessed in the Data Breach.

272. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

273. As a direct and proximate result of PSC's unfair acts and practices, Plaintiff and the Class have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or fraudulent use of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data

Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in PSC's possession (and/or to which PSC continues to have access) and is subject to further unauthorized disclosures so long as PSC fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed Private Information.

274. Neither Plaintiff nor the other Class members contributed to the Data Breach.

275. Plaintiff sent a demand for relief, in writing, to PSC on May 28, 2024, prior to filing this complaint. Multiple plaintiffs in consolidated actions have sent61—or alleged in their complaints that they would send62—similar demand letters as required by M.G.L. c. 93A § 9. Plaintiff has not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiff and the Class.

---

[61] *See, e.g., Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[62] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp*., 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al*., 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al*., 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al*., 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al*., 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al*., 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al*., 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al*., 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al*., 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Co., et al*., 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al*., 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al*., 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al*., 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al*., 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al.* , 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al*., 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp*., 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al*., 23-cv-1913 (D. Md.).

276. Based on the foregoing, Plaintiff and the other members of the class are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

277. Pursuant to M.G.L. ch. 231, § 6B, Plaintiff and other members of the Class are further entitled to pre-judgment interest as a direct and proximate result of PSC's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Plaintiff and other members of the Class are entitled to interest in an amount according to proof.

ELEVENTH CAUSE OF ACTION
DECLARATORY RELIEF. 28 U.S.C. § 2201
(On Behalf of Plaintiff and the Nationwide Class against PSC and CareSource)

278. Plaintiff realleges and incorporates by reference paragraphs 1-156 as if fully set forth herein.

279. An actual controversy has arisen and exists between Plaintiff and Class Members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and Class Members' Private Information, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and Class Members' Private Information from unauthorized access, disclosure, and use.

280. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect Private

Information is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there is clarity between the parties as to Defendants' data security obligations with respect to Private Information going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed National Class and the Ohio Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendants to delete and purge the PI of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendants to implement and maintain comprehensive Information Security Programs designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PI;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendants from maintaining Plaintiff's and Class Members' PI on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program

that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PI, as well as protecting the PI of Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

k. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendants to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Date: August 16, 2024

Respectfully submitted,

/s/ Karen H. Riebel

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

Michael R. Reese
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500
Email: *mreese@reesellp.com*

Charles D. Moore
REESE LLP
121 N. Washington Ave, 4th Floor
Minneapolis, Minnesota 55401
Telephone: 212-643-0500
Email: *cmoore@reesellp.com*

Counsel for Plaintiff